
ELabELN

Computer System Validation Manual

Installation Qualification (IQ) / Operational Qualification (OQ) / Performance Qualification (PQ)

Document Number	VLD-ELAB-001
Version	[] (Fill in at execution)
Effective Date	[] / [] / []
Document Status	DRAFT — Pending Validation Execution
Regulatory Basis	21 CFR Part 11 / GAMP 5 (Category 4)
System Name	ELabELN Electronic Laboratory Notebook
System Version	[] (Record installed version at time of IQ)
Deployment Model	LabServer (On-Premises) and/or sciCloud.net® (Cloud-Managed)
Supplier	LabLynx, Inc. www.lablynx.com support@lablynx.com

Powered by LabLynx, Inc.

www.lablynx.com | www.elabeln.com | support@lablynx.com

⚠ **CONFIDENTIAL — CONTROLLED DOCUMENT** ⚠

Table of Contents

Table of Contents	2
Document Control	3
Approval Signatures	3
Revision History	3
Distribution List	3
Section 1: Validation Overview	4
1.1 Purpose	4
1.2 Scope	4
1.3 Regulatory Basis	4
1.4 GAMP 5 Software Category Classification	5
1.5 System Description	5
1.6 Roles and Responsibilities	5
1.7 Risk Assessment and Test Depth Rationale	6
1.8 Acceptance Criteria	6
1.9 Deviation Handling	7
Section 2: System Configuration Baseline	8
2.1 Hardware Baseline (LabServer Deployments)	8
2.2 Software Baseline	8
2.3 Configuration Parameter Baseline	9
2.4 Interfaces Baseline	9
Section 3: Installation Qualification (IQ)	10
Section 4: Operational Qualification (OQ)	20
4.4 Authentication and Access Control [CRITICAL — 21 CFR 11.10(d), 11.300]	20
4.5 Experiment Management [HIGH]	25
4.6 Electronic Signatures [CRITICAL — 21 CFR Part 11 Subpart C: §11.50, §11.70, §11.100, §11.200, §11.300]	33
4.7 Trusted Timestamping [CRITICAL — 21 CFR 11.10(c), 11.70]	37
4.8 Audit Trail [CRITICAL — 21 CFR 11.10(e)]	39
4.9 Template Management [HIGH]	43
4.10 Resource Management [MEDIUM-HIGH]	45
4.11 User and Team Administration [HIGH]	46
4.12 System Configuration and Integration [MEDIUM]	48
4.13 OQ Summary	49
Section 5: Performance Qualification (PQ)	50
PQ-001: Complete Regulated Analytical Experiment Lifecycle	50
PQ-002: Multi-User Concurrent Access and Data Isolation	51
PQ-003: Template Enforcement Consistency Across Users	52
PQ-004: Audit Trail Integrity Under Sequential Edits by Multiple Users	53
PQ-005: Resource Traceability — Lot Impact Analysis	54
PQ-006: Backup and Restore Integrity	55
PQ-007: System Recovery After Unplanned Restart	57

PQ-008: API Integration — Programmatic Record Creation and Audit Trail	57
PQ-009: Data Archival and Long-Term Retrievability	58
PQ-010: Deviation and Incident Scenario — Post-Signature Modification Detection	59
5.2 PQ Summary	61
Section 6: Change Control and Revalidation Requirements	62
6.1 Change Control Trigger Criteria	62
Section 7: Validation Summary Report	63
7.1 Summary of Validation Results	63
7.2 21 CFR Part 11 Compliance Attestation	63
7.3 Final Approval and Release	64
Appendix A: 21 CFR Part 11 Traceability Matrix	65
Appendix B: Deviation Log Template	66
Appendix C: Abbreviations and Definitions	67
Appendix D: Referenced Documents	68

Document Control

Approval Signatures

Role	Name / Title	Signature / Date
Validation Owner	[Name / Title]	[Signature / Date]
Quality Assurance	[Name / Title]	[Signature / Date]
System Owner / IT	[Name / Title]	[Signature / Date]
Department Head	[Name / Title]	[Signature / Date]
Regulatory Affairs (if applicable)	[Name / Title]	[Signature / Date]

Revision History

Version	Description	Author / Date
1.0	Initial release — Version-agnostic baseline protocol.	[Author]
[]	[Description of change]	[Author]

Distribution List

Recipient	Copy Type
QA / Regulatory Affairs	Controlled Copy
Validation Owner	Controlled Copy
System Owner / IT	Controlled Copy
Department Head	Controlled Copy
Training Records Archive	Uncontrolled Reference Copy

Section 1: Validation Overview

1.1 Purpose

This document establishes the Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ) protocols for ELabELN, an Electronic Laboratory Notebook (ELN) system delivered by LabLynx, Inc. The purpose of this validation is to provide documented evidence that ELabELN has been correctly installed, operates as intended within its specified functional requirements, and performs reliably in the actual user environment — in full compliance with 21 CFR Part 11 requirements for electronic records and electronic signatures.

1.2 Scope

This validation covers ELabELN as deployed in the following configurations:

- LabServer Deployment: On-premises installation on Ubuntu Server 24.04 LTS using Docker Engine and Docker Compose, as documented in the ELabELN License, Technical Specifications & Installation Manual.
- sciCloud.net® Cloud Deployment: LabLynx-managed hosted deployment on the sciCloud.net® platform (AWS-based), where LabLynx is responsible for infrastructure qualification.

The validation covers all features and functions of ELabELN that support electronic records and electronic signatures subject to 21 CFR Part 11, including: user authentication, access control, audit trail, electronic signatures, trusted timestamping, experiment management, template enforcement, resource management, and the administrative configuration required to maintain system integrity.

Note

For sciCloud.net® deployments, the infrastructure-level IQ (server hardware, OS, Docker platform, network, backups) is the responsibility of LabLynx, Inc. and is covered by LabLynx's infrastructure qualification documentation. Customers using sciCloud.net® execute the Application IQ, full OQ, and full PQ as documented here.

1.3 Regulatory Basis

Regulation / Guidance	Relevance and Application
21 CFR Part 11	FDA regulation governing electronic records and electronic signatures. This is the primary regulatory driver for this validation. All critical controls tested in the OQ are mapped to specific Part 11 subsections.
GAMP 5 (2nd Edition)	Risk-based approach to computer system validation. ELabELN is classified as GAMP 5 Category 4 (Configurable Software). This classification establishes the validation strategy: full IQ, OQ, and PQ with risk-proportionate test depth.
FDA Guidance — Part 11, ERR, ES (2003)	FDA's guidance document on the scope and application of 21 CFR Part 11. This document confirms that predicate rule records documented in ELabELN must meet all Part 11 requirements.
FDA Guidance — Computerized Systems in Clinical Investigations (1999)	Applicable to any clinical investigation records maintained in ELabELN.
ICH Q9 — Quality Risk Management	Provides the framework for the risk assessment used to prioritize OQ test depth.

ISO/IEC 62304	Referenced for software lifecycle documentation (applicable if ELabELN is used in a medical device quality system context).
----------------------	---

1.4 GAMP 5 Software Category Classification

ELabELN is classified as GAMP 5 Category 4 — Configurable Software. Category 4 software is commercially available software that is configured by the customer (via templates, settings, user groups, workflows) but not custom-programmed. The implications for validation scope are:

- IQ: Verify the software is installed as specified, with the correct version and configuration.
- OQ: Verify all configured functions operate according to their specifications (full test coverage required per the instructions for this document).
- PQ: Verify the configured system performs correctly in actual use under representative real-world conditions.
- Supplier Audits: LabLynx is the supplier. The GAMP 5 framework recommends supplier assessment, which LabLynx supports through its SOC 2 compliance documentation, security policies, and technical support.

1.5 System Description

Attribute	Value
System Name	ELabELN Electronic Laboratory Notebook
Supplier	LabLynx, Inc., Pensacola, Florida, USA
Supplier Contact	support@lablynx.com www.lablynx.com
Underlying Platform	eLabFTW (open-source ELN, Deltablot SAS, AGPL-3.0)
System Version	[Record installed version: _____]
Deployment Model	LabServer (on-premises) and/or sciCloud.net® (cloud-managed)
Operating System (LabServer)	Ubuntu Server 24.04 LTS (64-bit x86_64)
Container Runtime (LabServer)	Docker Engine 27.x with Docker Compose plugin v2.x
Database	MySQL 8.4.x (containerized via Docker)
Web Server (inside container)	nginx 1.26.x + PHP-FPM 8.3.x
Primary URL	https://[your-elabeln-domain.com]
Intended Use	Electronic laboratory notebook for creation, management, and electronic signing of scientific records subject to 21 CFR Part 11 controls.
GxP Impact	High — Records maintained in ELabELN may directly support regulatory submissions, clinical investigations, GMP batch records, or GLP study records.

1.6 Roles and Responsibilities

Role	Responsibility
Validation Owner	Responsible for the overall validation effort: planning, coordination, final sign-off, and maintenance. Typically a QA or Regulatory Affairs manager.

Test Executor(s)	Personnel who perform the IQ, OQ, and PQ test steps and record actual results. Must be trained on ELabELN. Must sign and date each test record at execution.
QA Reviewer	Reviews and approves all test protocols and completed test records. Confirms pass/fail determinations are appropriate. Signs off on the Validation Summary Report.
System Owner / IT (LabServer)	Responsible for infrastructure qualification (server, OS, Docker). Executes and signs off on hardware/OS/infrastructure IQ steps.
LabLynx Support	Provides product specifications, release notes, and technical clarifications. Does not execute validation tests on behalf of the customer but may provide advisory support.
End Users	Participate in PQ scenario execution under the supervision of the Validation Owner and QA Reviewer. Represent real-world operating conditions.

1.7 Risk Assessment and Test Depth Rationale

Per GAMP 5 and ICH Q9, the depth of testing is proportional to the risk of incorrect system function. The following risk classification drives test protocol depth in this document:

Risk Level	Function Categories	Testing Approach
CRITICAL	Electronic signatures, audit trail, session authentication, access control, record integrity (lock/immutability), trusted timestamping.	Full step-by-step test scripts. Testing must confirm both the positive case (function works) and the negative case (attempt to circumvent fails).
HIGH	Experiment creation/management, template enforcement, metadata fields, file attachments, export functions, user/team management, notifications.	Full step-by-step test scripts. Positive-case testing required.
MEDIUM	Resource management, scheduler, tag management, search functions, batch actions, API authentication.	Full step-by-step test scripts. Representative test cases for each function type.
LOW	UI display preferences, non-compliance-affecting cosmetic settings, developer tools.	Not explicitly tested in OQ. Verified as part of PQ scenarios if encountered.

1.8 Acceptance Criteria

The overall validation is considered successful when:

- All IQ test cases receive a Pass result, or all failures have documented deviations with approved CAPAs.
- All OQ test cases at CRITICAL or HIGH risk receive a Pass result, or all failures have documented deviations with approved CAPAs.
- All OQ test cases at MEDIUM risk receive a Pass result, or all failures have documented deviations.
- All PQ scenarios receive a Pass result, or all failures have documented deviations with approved CAPAs.
- The Validation Summary Report (Section 7) is reviewed by QA and signed by all required approvers.

Important

Any OQ test case in the CRITICAL category (electronic signatures, audit trail, access control, record integrity) that fails without an acceptable documented resolution must result in the system being placed in a restricted-use hold. The system must not be used for GxP records until the deviation is resolved, retested, and approved.

1.9 Deviation Handling

If any test step produces an Actual Result that does not match the Expected Result, the following procedure applies:

1. Record the actual result observed in the Actual Result column. Do not alter the Expected Result.
2. Mark the test step as FAIL in the P/F column.
3. Open a Deviation Record (Appendix D template) immediately. Assign a deviation number.
4. Classify the deviation: Critical (prevents system use for GxP records), Major (affects primary function but has a workaround), or Minor (cosmetic, does not affect GxP record integrity).
5. Initiate a CAPA if the deviation is Critical or Major. The CAPA must be approved by QA before retesting.
6. After CAPA implementation, retest the failed step(s). Document the retest result on the Deviation Record.
7. Include all deviations and their resolutions in the Validation Summary Report (Section 7).

Section 2: System Configuration Baseline

Complete this section at the time of validation execution. The values recorded here become the approved configuration baseline. Any subsequent change to these values requires a formal change control and re-validation assessment.

2.1 Hardware Baseline (LabServer Deployments)

Hardware Component	Recorded Value
Server Make / Model	[]
CPU Architecture	x86_64 (64-bit) — Cores: [] Threads: []
Total RAM Installed	[] GB
Operating System	Ubuntu Server 24.04 LTS (Noble Numbat)
OS Kernel Version	[Record: uname -r output: _____]
Primary Data Disk Size	[] GB — Mount: /var/elabftw
Network Interface	IP Address: [] Hostname: []
Server Location / Data Center	[]

Note

For sciCloud.net® deployments, replace this table with: 'Infrastructure qualification is the responsibility of LabLynx, Inc. Reference: LabLynx Infrastructure Qualification Document IQ-INFRA-[version], on file with LabLynx and available to customers upon request.'

2.2 Software Baseline

Software Component	Recorded Version
Docker Engine Version	[Record: docker version output: _____]
Docker Compose Plugin Version	[Record: docker compose version output: _____]
ELabELN Image Tag	[Record: docker inspect elabftw --format '{{.Config.Image}}': _____]
ELabELN Image Digest (SHA256)	[Record: docker inspect elabftw --format '{{.Image}}': _____]
MySQL Image Tag	[Record: docker inspect mysql --format '{{.Config.Image}}': _____]
MySQL Image Digest (SHA256)	[Record: docker inspect mysql --format '{{.Image}}': _____]
ELabELN Application Version	[Record: docker exec elabftw bin/init system:info grep version: _____]
PHP Version	[Record: docker exec elabftw php -r 'echo PHP_VERSION;': _____]

nginx Version	[Record: docker exec elabftw nginx -v: _____]
MySQL Server Version	[Record: docker exec mysql mysql -u elabftw -p -e 'SELECT VERSION();': ____]

2.3 Configuration Parameter Baseline

Configuration Parameter	Recorded Value
SITE_URL (docker-compose.yml)	[Record value: _____]
SERVER_NAME	[Record value: _____]
PHP_TIMEZONE / TZ	[Record value: _____]
ENABLE_LETSENCRYPT	true / false (circle one)
DISABLE_HTTPS	true / false (circle one)
PHP_MAX_CHILDREN	[Record value: _____]
MAX_PHP_MEMORY	[Record value: _____]
MAX_UPLOAD_SIZE	[Record value: _____]
USE_REDIS	true / false (circle one)
AUTO_DB_INIT	true / false (circle one)
AUTO_DB_UPDATE	true / false (circle one)
MFA Enforcement (Admin Panel)	Enabled / Disabled (circle one)
SSO / LDAP Configured	Yes / No (circle one) — Provider: [_____]
RFC 3161 TSA Configured	Provider: [_____] URL: [_____ _____]

2.4 Interfaces Baseline

Interface	Configuration Record
SMTP Email Server	Host: [_____] Port: [____] TLS: Yes/No Auth: Yes/No
SSO / SAML Identity Provider	[Provider name / URL or N/A: _____]
LDAP Directory Server	[Host / Base DN or N/A: _____]
RFC 3161 Timestamp Authority	[Provider / URL: _____]
ELab LIMS Integration	Yes / No — API endpoint: [_____]
REST API External Clients	[List active API integrations or 'None': _____]

Section 3: Installation Qualification (IQ)

The Installation Qualification verifies that ELabELN has been correctly installed in the target environment, that all components match their approved specifications, and that the system is ready for Operational Qualification testing. The IQ must be completed and approved before any OQ testing begins.

IQ Scope Note — LabServer vs. sciCloud.net®

LabServer (on-premises): All IQ tests (IQ-001 through IQ-014) apply.
sciCloud.net® (cloud): IQ-001 through IQ-006 (infrastructure) are pre-qualified by LabLynx. Customers execute IQ-007 through IQ-014 (application configuration, accessibility, database). Mark IQ-001–IQ-006 as 'N/A — LabLynx Infrastructure IQ' and attach LabLynx's IQ evidence package.

IQ-001 Host Operating System Verification

21 CFR Part 11 Reference: 21 CFR 11.10(a) — System controls to ensure record authenticity and integrity begin at the OS level.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Must be performed by IT/System Owner. Requires SSH or console access to the Ubuntu server. For sciCloud.net®, mark N/A and attach LabLynx IQ evidence.						
1	Log in to the Ubuntu server via SSH or local console.	Successful login as authorized user.				
2	Execute: <code>lsb_release -a</code>	Output shows: Ubuntu 24.04.x LTS Noble Numbat 64-bit.				
3	Execute: <code>uname -m</code>	Output shows: x86_64				
4	Execute: <code>uname -r</code>	Record the kernel version in Section 2.1. Version is 6.x.x or later.				
5	Execute: <code>df -h /var/elabftw</code>	Mount point /var/elabftw (or equivalent data volume) exists with sufficient free space (minimum 20 GB available).				
6	Execute: <code>sudo systemctl status docker</code>	Docker service status is 'active (running)'. Docker is enabled for boot: <code>sudo systemctl is-enabled docker</code> returns 'enabled'.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

IQ-002 Docker Engine Version Verification

21 CFR Part 11 Reference: 21 CFR 11.10(b) — Software must meet all applicable requirements to generate records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Confirm Docker was installed from the official Docker CE repository, not via snap.						
1	Execute: docker version	Output shows Docker Engine version 27.x.x or later for both Client and Server. No error messages.				
2	Execute: docker compose version	Output shows Docker Compose version v2.x.x or later.				
3	Execute: docker info grep 'Storage Driver'	Output shows overlay2 as the storage driver (not vfs).				
4	Execute: which docker	Output shows /usr/bin/docker (not /snap/bin/docker). If snap path appears, Docker must be reinstalled from official repository.				
5	Execute: docker run --rm hello-world	Output includes 'Hello from Docker!' confirming container runtime is functional.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-003 Container Image Version Verification

21 CFR Part 11 Reference: 21 CFR 11.10(b) — All applicable software requirements must be met.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Both containers (elabftw and mysql) must be running before this test. Execute 'cd /etc/elabftw && sudo docker compose up -d' if not already running.						
1	Execute: docker ps --format '{{.Names}}\t{{.Image}}\t{{.Status}}'	Output lists both 'elabftw' and 'mysql' containers as 'Up' with healthy status.				
2	Execute: docker inspect elabftw --format '{{.Config.Image}}'	Output shows the approved image tag (e.g., elabftw/elabimg:stable or pinned version). Record value in Section 2.2.				
3	Execute: docker inspect elabftw --format '{{.Image}}'	Output shows a SHA256 image digest. Record this value in Section 2.2 as the immutable image fingerprint.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Execute: docker inspect mysql --format '{{.Config.Image}}'	Output shows mysql:8.4 or approved pinned version. Record in Section 2.2.				
5	Execute: docker inspect mysql --format '{{.Image}}'	Output shows a SHA256 digest. Record in Section 2.2.				
6	Execute: docker exec elabftw bin/init system:info grep -i version	ELabELN application version is displayed. Record in Section 2.2.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

IQ-004 Data Persistence Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(c) — Computer-generated audit trails must be protected from modification or deletion.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: The /var/elabftw/web and /var/elabftw/mysql directories must exist on the host before running this test.						
1	Execute: docker inspect elabftw --format '{{json .Mounts}}' python3 -m json.tool	Output shows two volume mounts: (1) host /var/elabftw/web mapped to container /elabftw/uploads; (2) host /var/elabftw/mysql mapped to container /var/lib/mysql.				
2	Execute: ls -la /var/elabftw/web	Directory exists and is owned by UID 101 (nginx user). Permissions are 750 or 755.				
3	Execute: ls -la /var/elabftw/mysql	Directory exists and contains MySQL data files. Not empty (indicating MySQL has initialized).				
4	Execute: docker exec elabftw stat /elabftw/uploads	Command returns file system information confirming the uploads directory is accessible inside the container.				
5	Execute: docker exec mysql ls /var/lib/mysql	Directory is accessible and contains MySQL database files.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-005 Network Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(d) — System access must be limited to authorized individuals.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Verify that the MySQL container is not exposed externally and that only port 443 (HTTPS) is exposed to the host network.						
1	Execute: docker network ls	Output includes elabftw_elabftw-net (the internal bridge network). Record network name.				
2	Execute: docker network inspect elabftw_elabftw-net --format '{{range .Containers}}{{.Name}}{{end}}'	Output lists both 'elabftw' and 'mysql' as members of the internal network.				
3	Execute: docker ps --format '{{.Names}}\t{{.Ports}}'	'elabftw' shows 0.0.0.0:443->443/tcp (or 127.0.0.1:443). 'mysql' shows NO external port mapping (only internal 3306/tcp exposed).				
4	From an external client (not the server), attempt: curl -k https://[SERVER_IP]/api/v2/info	Returns HTTP 200 with JSON content. The ELabELN application is accessible over HTTPS.				
5	From an external client (not the server), attempt TCP connection to port 3306: nc -zv [SERVER_IP] 3306	Connection is refused or times out. MySQL port is NOT accessible from outside the server.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-006 TLS Certificate Verification

21 CFR Part 11 Reference: 21 CFR 11.10(d) — Access controls; 21 CFR 11.30 — Open networks require encryption.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: TLS (HTTPS) must be operational before any electronic records are created. This test verifies the certificate is valid, not expired, and matches the configured server name.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	Execute: <code>echo openssl s_client -connect [SERVER_NAME]:443 -servername [SERVER_NAME] 2>/dev/null openssl x509 -noout -subject -dates</code>	Output shows: subject with CN=[SERVER_NAME]; notBefore and notAfter dates. notAfter must be a future date (at least 30 days from now).				
2	Navigate to <code>https://[SERVER_NAME]</code> in a browser (Chrome or Firefox).	Browser shows a secure padlock icon. No certificate warning is displayed. The address bar shows <code>https://</code> protocol.				
3	Execute: <code>curl -I https://[SERVER_NAME]/</code>	Response headers include: HTTP/2 200, Strict-Transport-Security header present.				
4	Attempt to navigate to <code>http://[SERVER_NAME]/</code> (HTTP, not HTTPS).	Browser is redirected to HTTPS, or connection is refused. Plain HTTP access to application data is not permitted.				
5	Execute: <code>echo openssl s_client -connect [SERVER_NAME]:443 2>/dev/null grep 'Protocol'</code>	Protocol shows TLSv1.2 or TLSv1.3 only. Protocols TLSv1.0 and TLSv1.1 must NOT appear.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

IQ-007 Database Initialization and Schema Verification

21 CFR Part 11 Reference: 21 CFR 11.10(a) — Validation to ensure accuracy, reliability, consistent intended performance.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: The database must have been initialized via ' <code>docker exec elabftw bin/init db:install</code> ' before this test.						
1	Execute: <code>docker exec mysql mysql --user=elabftw --password=[DB_PASSWORD] elabftw --execute='SHOW TABLES;'</code>	Output lists ELabELN database tables (experiments, items, users, audit_logs, etc.). No empty result. Record number of tables displayed: [_____]				
2	Execute: <code>docker exec mysql mysql --user=elabftw --password=[DB_PASSWORD] elabftw</code>	Returns a count greater than 0, confirming the configuration table is populated.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	--execute='SELECT COUNT(*) FROM config;'					
3	Execute: docker exec elabftw bin/init db:updatecheck	Output confirms the database schema is current for the installed version (no pending updates required, or updates have been applied).				
4	Execute: docker exec elabftw bin/init system:info	Output displays system information without errors. All checks shown are green/OK.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-008 Application Accessibility Verification

21 CFR Part 11 Reference: 21 CFR 11.10(b) — Software must generate accurate and complete records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Open a supported browser (Chrome 120+ or Firefox 120+). Navigate to the ELabELN instance URL.						
1	Navigate to https://[SERVER_NAME]/	The ELabELN login page loads completely. The LabLynx/ELabELN branding is visible. No error messages or broken elements.				
2	Navigate to https://[SERVER_NAME]/api/v2/info	Returns a JSON response containing the ELabELN version string and other system information. HTTP status code 200.				
3	Attempt to navigate to https://[SERVER_NAME]/api/v2/experiments without an API key.	Returns HTTP status 401 (Unauthorized). The API does not grant access without authentication.				
4	Navigate to https://[SERVER_NAME]/app/logout.php	Redirects to the login page without error. Session termination is handled gracefully.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-009 Email Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(b) — Supporting features (notifications) must function as specified.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: SysAdmin account required. Log in to ELabELN as SysAdmin before running this test.						
1	Log in as SysAdmin. Navigate to User Avatar → Sysconfig → Email tab.	The Email configuration page loads. SMTP settings (host, port, from address, authentication) are populated with the approved values from Section 2.4.				
2	Click the 'Send test email' button. Provide a valid recipient email address.	A test email is received at the specified address within 5 minutes. Subject line contains 'ELabELN' or similar identifier.				
3	Verify email content.	The test email body confirms the sender is the configured from-address. No SMTP authentication errors appear in the system logs.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-010 Backup System Verification

21 CFR Part 11 Reference: 21 CFR 11.10(c) — Protection of records to enable accurate and ready retrieval throughout records retention period.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A backup procedure must have been configured per the Installation Manual before this test. For sciCloud.net®, LabLynx performs backup verification; attach LabLynx backup attestation and mark this test N/A.						
1	Execute the configured backup command (e.g., sudo elabctl backup run or sudo /usr/local/bin/elab-backup.sh).	Backup completes without error. Backup output or log confirms: (a) database dump was created; (b) uploads directory was copied.				
2	Navigate to the backup destination directory. Verify the following files exist: database dump file (.sql.gz or equivalent); uploads backup (directory or archive); docker-compose.yml backup.	All three backup elements are present, timestamped with today's date, and non-zero in size.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
3	Verify the scheduled backup task (cron job or systemd timer) is active.	Execute: crontab -l or cat /etc/cron.d/elab* shows an active scheduled backup task. Backup is scheduled to run at a defined interval (minimum daily).				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____

IQ-011 Log Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(e) — Audit trails must be generated and retained.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Verify that container logs are configured with appropriate retention and that ELabELN application logs are accessible.						
1	Execute: cat /etc/docker/daemon.json	File contains log-driver: json-file with max-size and max-file settings. Log rotation is configured.				
2	Execute: sudo docker logs elabftw --tail 20	Returns the most recent nginx and PHP-FPM log entries without error.				
3	Execute: sudo docker logs mysql --tail 20	Returns the most recent MySQL log entries without error. No critical error messages visible.				
4	Verify logrotate is configured: cat /etc/logrotate.d/docker-elabftw	Logrotate configuration file exists with rotate, daily, and compress settings.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____

IQ-012 Security Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(d) — Limiting system access to authorized individuals; 21 CFR 11.300 — Controls for identification codes/passwords.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Verify host-level security hardening has been applied per the Installation Manual (Security Hardening chapter).						
1	Execute: sudo ufw status verbose	ufw is active. Rules show: port 22 (SSH), 443 (HTTPS), and optionally 80 (HTTP) are allowed. No unnecessary ports are open.				
2	Execute: sudo systemctl status fail2ban	fail2ban service is 'active (running)'. Execute: sudo fail2ban-client status. Shows active jails including sshd.				
3	Execute: sudo systemctl status unattended-upgrades	Service is active (running) or enabled. Automatic security updates are configured.				
4	Execute: ls -la /etc/elabftw/docker-compose.yml	File permissions are 600 (owner read/write only). File is owned by root.				
5	Verify SSH key authentication is required: cat /etc/ssh/sshd_config grep PasswordAuthentication	PasswordAuthentication is set to 'no'. PermitRootLogin is 'no'.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

IQ-013 SysAdmin Account and Initial Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(d) — System access limited to authorized individuals; 21 CFR 11.300 — Identification codes/passwords.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Log in to ELabELN as SysAdmin. The first account created on a fresh installation automatically receives SysAdmin privileges.						
1	Navigate to https://[SERVER_NAME]/. Attempt to access the login page.	Login page is displayed. No error messages.				
2	Log in with SysAdmin credentials (email + password).	Login is successful. User is redirected to the ELabELN dashboard. The username/email is displayed in the top-right corner.				
3	Navigate to User Avatar → Sysconfig.	The Sysconfig panel opens successfully. All configuration tabs (Users, Teams, Email,				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
		Security, Authentication, Timestamping, API) are visible.				
4	Navigate to Sysconfig → Security. Verify the password policy settings match the organization's approved policy.	Password minimum length and complexity settings reflect the organization's approved security policy.				
5	Navigate to Sysconfig → Users. Confirm that only authorized accounts exist (no unexpected accounts).	User list contains only expected, authorized accounts.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

IQ-014 IQ Summary and Release for OQ

21 CFR Part 11 Reference:

IQ Summary Item	Recorded Value
Total IQ Tests	14
Tests Passed	[Record: _____]
Tests Failed	[Record: _____]
Tests Not Applicable (N/A)	[Record: _____] — (List N/A IDs: _____)
Open Deviations	[Record: _____] — (List Deviation IDs: _____)
IQ Overall Result	PASS / FAIL / CONDITIONAL PASS (circle one)
Conditional Pass Conditions	[Describe any conditions required before OQ commencement: _____]

Role	Name	IQ Approval Signature / Date
Validation Owner	[Name / Title]	[Signature / Date]
QA Reviewer	[Name / Title]	[Signature / Date]

Section 4: Operational Qualification (OQ)

The Operational Qualification verifies that ELabELN operates according to its functional specifications across all system functions. Each test protocol below documents exact procedural steps, expected results, and record fields for actual results, pass/fail determination, tester initials, and execution date.

OQ Prerequisites: (1) IQ is complete and approved. (2) At least two test user accounts exist with different roles (regular User and Admin). (3) At least one team is configured. (4) Test browsers are supported versions (Chrome 120+ or Firefox 120+). (5) A test experiment template with at least 3 metadata fields and 3 steps (including 1 locked step) has been created by the Admin.

21 CFR Part 11 Reference

The OQ test cases in Sections 4.4 (Authentication/Access Control), 4.6 (Electronic Signatures), 4.7 (Timestamps), and 4.8 (Audit Trail) are CRITICAL under 21 CFR Part 11 requirements. All other sections are HIGH or MEDIUM risk. All test cases in this document require full detailed execution per instructions provided.

4.4 Authentication and Access Control [CRITICAL — 21 CFR 11.10(d), 11.300]

OQ-AC-001 Local Authentication — Valid Credentials

21 CFR Part 11 Reference: 21 CFR 11.10(d): Limit system access to authorized individuals; 21 CFR 11.300(a): Unique identifiers.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use a test account with a known valid password. Ensure the account is active and validated.						
1	Navigate to https://[SERVER_NAME]/ . Observe the login page.	The login page displays fields for Email and Password. A company/LabLynx logo is visible. No authenticated content is visible without login.				
2	Enter the valid test user email and correct password. Click Sign In.	Login succeeds. User is redirected to their ELabELN dashboard. The user's name appears in the top-right navigation. No error messages are displayed.				
3	Observe the browser URL bar after successful login.	URL contains /experiments or similar authenticated path. No session token is visible in the URL (tokens are handled via HTTP cookies, not URL parameters).				
4	Log out by clicking User Avatar → Sign Out.	User is redirected to the login page. The session is terminated.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
5	Attempt to navigate directly to https://[SERVER_NAME]/app/experiments.php (a protected page) after logout.	User is redirected back to the login page. Unauthenticated access to protected pages is not permitted.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

OQ-AC-002 Authentication — Invalid Credentials and Account Lockout

21 CFR Part 11 Reference: 21 CFR 11.300(c): Use of appropriate controls (e.g., password or token systems) to limit unauthorized access.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use a test account. Note: this test will lock the account temporarily. Have the SysAdmin password available to unlock if needed.						
1	Navigate to the login page. Enter the test user email with an incorrect password. Click Sign In.	Login fails. An error message is displayed (e.g., 'Invalid credentials'). No information about whether the account exists is leaked.				
2	Repeat the incorrect password entry 5 consecutive times (or the configured lockout threshold from Section 2.3).	After the configured number of failures, the account is temporarily locked. A message or behavior change confirms the lockout.				
3	Wait the configured lockout duration (e.g., 15 minutes as configured in fail2ban). Attempt login with the correct password.	Login succeeds after the lockout period expires, confirming lockout is temporary rather than permanent.				
4	As SysAdmin, verify login attempt events are recorded. Navigate to Sysconfig → Logs and filter for authentication events.	Failed login attempts appear in the system audit log with timestamp and IP address. Successful login after unlock also appears.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

OQ-AC-003 Multi-Factor Authentication (MFA) Enforcement

21 CFR Part 11 Reference: 21 CFR 11.300(b),(d): Operational checks to ensure valid users; two-factor controls.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: MFA must be configured for the test account before running this test. Admin Panel → Team tab → Force MFA must be enabled, or the test user must have voluntarily enrolled. Use an authenticator app (Google Authenticator, Authy, Aegis, or equivalent).						
1	Navigate to the login page. Enter the MFA-enrolled test user email and correct password. Click Sign In.	After password validation, the system presents a second challenge: a prompt for the 6-digit MFA code.				
2	Enter an incorrect 6-digit code (e.g., 000000). Click Verify.	Authentication fails. Error message indicates the code is invalid. The user remains on the MFA challenge page.				
3	Open the authenticator app. Retrieve the current 6-digit TOTP code for the enrolled account. Enter it in the MFA challenge prompt.	Authentication succeeds. User is redirected to their dashboard.				
4	Verify the MFA event appears in the system audit log. As SysAdmin, navigate to Sysconfig → Logs.	Successful MFA authentication event is recorded with timestamp, user identity, and IP address.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-AC-004 Session Timeout Enforcement

21 CFR Part 11 Reference: 21 CFR 11.10(d): Time-limited access; session controls.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Configure a short session timeout (e.g., 5 minutes) temporarily in the SysAdmin panel for testing purposes. Restore the production value after the test.						
1	Log in as a test user. Note the login time.	Successful login. Record start time: []				
2	Leave the browser idle (do not perform any actions) for the duration of the configured session timeout period.	[Wait configured timeout + 2 minutes]				
3	After the timeout period has elapsed, attempt to perform an action (e.g., click Experiments in the navigation bar).	User is redirected to the login page. The session has expired. A message may indicate the session timed out.				
4	Verify that no data entered before the timeout is	Login page is presented. No ELabELN content is				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	accessible without re-authentication.	accessible without fresh authentication.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

OQ-AC-005 Role-Based Access Control — User Cannot Access Admin Panel

21 CFR Part 11 Reference: 21 CFR 11.10(d): System access limited to authorized individuals only.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Log in as a standard User (not Admin, not SysAdmin) for this test.						
1	Log in as a standard User. Click the User Avatar (top right).	The dropdown menu does NOT display 'Admin Panel' or 'Sysconfig' options. Only personal settings options are visible.				
2	Attempt to navigate directly to the Admin Panel URL: https://[SERVER_NAME]/app/admin.php	Access is denied. User receives an error page or is redirected. The Admin Panel content is NOT displayed.				
3	Attempt to navigate directly to the SysAdmin URL: https://[SERVER_NAME]/app/sysconfig.php	Access is denied. User receives an error page or is redirected. The SysAdmin content is NOT displayed.				
4	As the User, attempt to create a new experiment category (a function reserved for Admins).	The option to create a new category is not available in the User's interface. No unauthorized category creation is possible.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

OQ-AC-006 Permission Model — Private Experiment Not Visible to Other Users

21 CFR Part 11 Reference: 21 CFR 11.10(d): Access controls to protect records from unauthorized access.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Two test user accounts (User A and User B) in the same team are required. Both must be logged in on separate browser sessions.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	Log in as User A. Create a new experiment titled 'AC-006 Private Test — Do Not Share'. Set visibility to 'Only Me (Private)'. Save.	'Only Me' visibility setting is accepted. Experiment is saved and visible to User A.				
2	As User A, note the experiment's ELabID and URL from the browser address bar.	Record ELabID: [] URL: []				
3	In a separate browser (or incognito window), log in as User B. Navigate to Experiments index. Search for the experiment title 'AC-006 Private Test — Do Not Share'.	'Only Me' experiment does NOT appear in User B's search results.				
4	As User B, attempt to navigate directly to the experiment URL noted in Step 2.	Access is denied. User B receives a 403 Forbidden error or is redirected to the experiments index. The experiment content is NOT displayed.				
5	As User A, change the experiment's visibility to 'My Team'. As User B, refresh the experiments index and search again.	The experiment is now visible to User B in the index.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
------------------------	----------------	--	-----------------------

OQ-AC-007 Account Deactivation — Immediate Access Revocation

21 CFR Part 11 Reference: 21 CFR 11.10(d): Limit access to currently authorized individuals; deactivation controls.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A test account to be deactivated and an active SysAdmin account are required. Ensure the test account data has been backed up or ownership transferred before deactivation.						
1	Log in as the SysAdmin. Navigate to Sysconfig → Users. Locate the test account. Set the account's validity expiry date to yesterday's date (or set the account to Inactive). Save.	Account is marked as expired/inactive in the Users list.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
2	In a separate browser, attempt to log in with the deactivated test account credentials.	Login fails immediately. An error message indicates the account is not active or access is denied. The user is NOT granted any access.				
3	Confirm any active session from the deactivated account (if one existed before deactivation) is also terminated. Refresh the browser for the deactivated user if a session was open.	Existing session shows an authentication error or the user is redirected to the login page.				
4	As SysAdmin, verify the deactivation event is recorded in the audit log.	Sysconfig → Logs shows the account modification event with timestamp and SysAdmin identity.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

4.5 Experiment Management [HIGH]

OQ-EX-001 Experiment Creation — From Template

21 CFR Part 11 Reference: 21 CFR 11.10(b): Software meets all applicable requirements for generating records accurately and completely.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A test template with at least 3 metadata fields and 3 steps (one locked) must exist. Log in as a regular User.						
1	Navigate to Experiments → Create. Select the test template from the template dropdown. Click Create.	New experiment is created. The experiment opens in edit mode. The body text, metadata fields, and steps from the template are pre-populated.				
2	Observe the metadata fields.	All metadata fields from the template are present: correct names, correct field types (text, number, date, select, etc.), and any default values.				
3	Observe the Steps checklist.	All steps from the template are present in the correct order. The locked step has a lock icon and is not editable.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Attempt to edit the locked step's description text (click on it and try to type).	The locked step text is read-only. No modification is accepted.				
5	Enter a title: 'OQ-EX-001 Template Test'. Fill in at least one metadata field. Click Save.	Experiment is saved. No error messages. The experiment appears in the Experiments index.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____

OQ-EX-002 Experiment Category and Status Assignment

21 CFR Part 11 Reference: 21 CFR 11.10(b): Records must reflect correct classification information.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Open experiment OQ-EX-001 from the previous test, or create a new blank experiment.						
1	In edit mode, locate the Category field. Select a category from the dropdown.	Category is assigned. The category label appears with its configured color in the experiment header.				
2	Locate the Status field. Change the status from the default ('Running' or configured default) to a different status.	Status is updated. The new status label appears with its configured color.				
3	Save the experiment. Navigate back to the Experiments index.	The experiment appears in the index with the correct category color badge and status label.				
4	In the index, filter by the category assigned in Step 1.	Only experiments of that category are shown. The test experiment is visible in the filtered list.				
5	Filter by the status assigned in Step 2.	Only experiments with that status are shown. The test experiment is visible.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____

OQ-EX-003 Custom Metadata Fields — All Field Types

21 CFR Part 11 Reference: 21 CFR 11.10(b): Records must accurately capture all required data elements.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Create a new blank experiment. Use the Admin-configured test template that has at least one field of each type: text, number, date, select/dropdown, checkbox.						
1	In the metadata section, locate the Text field. Type: 'Test Analyst JR'. Click Save.	Text field value 'Test Analyst JR' is saved and displayed correctly on the next page load.				
2	Locate the Number field (with units). Enter: 99.3. Select unit 'mg/mL'. Click Save.	Number value 99.3 and unit mg/mL are saved and displayed correctly.				
3	Locate the Date field. Use the date picker to select today's date. Click Save.	Today's date is saved and displayed in YYYY-MM-DD format.				
4	Locate the Select (dropdown) field. Select an option (e.g., 'Pass'). Click Save.	The selected option is saved and displayed correctly.				
5	Locate the Checkbox field. Click it to check it. Click Save.	Checkbox is shown as checked/enabled after save.				
6	Switch to View mode. Verify all field values are displayed correctly.	All metadata field values entered in steps 1–5 are visible in view mode with correct labels and values.				
7	Clear the Number field entirely and click Save.	Empty numeric field is accepted without causing an application error.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-EX-004 Experiment Steps — Completion with Timestamp Attribution

21 CFR Part 11 Reference: 21 CFR 11.10(e): Audit trails must include date/time stamps and user identification for all steps.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Open the experiment created in OQ-EX-001. The experiment must have at least one unlocked step.						
1	In edit mode, locate the Steps checklist. Note the current state of an unlocked step (unchecked).	Unchecked step is visible with a checkbox on the left.				
2	Click the checkbox on an unlocked step.	The step is immediately marked as complete. A				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
		timestamp and the current user's name/initials appear next to the step completion. The next incomplete step advances.				
3	Switch to View mode. Observe the completed step.	Completed step shows a check mark, the user's name (or initials), and the exact date and time of completion.				
4	Navigate to the Experiments index. Observe the experiment row.	The experiment row shows the next incomplete step (if any remain) as a reminder in the Next Step column.				
5	Navigate to the To-Do List (top-left navigation icon).	The To-Do list shows remaining incomplete steps for this experiment and all other open experiments owned by the current user.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-EX-005 File Attachment Upload and Retrieval

21 CFR Part 11 Reference: 21 CFR 11.10(b): Records must include all required supporting data; original data retention.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Prepare a test file for upload (e.g., a small PDF or text file named 'OQ-EX-005-testfile.pdf').						
1	Open a test experiment in edit mode. Locate the Attachments section. Drag the test file onto the upload area (or click Browse and select it).	File upload progress is displayed. After completion, the file appears in the Attachments panel with its name, size, upload timestamp, and uploader identity.				
2	Switch to View mode. Observe the attachment entry.	File is listed in the Attachments panel with: filename, file size, upload date and time, and the name of the user who uploaded it.				
3	Click on the attachment to download it.	File downloads correctly. The downloaded file is identical to the original uploaded file (not corrupted, not renamed).				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Attempt to upload a second file with the same name.	System either renames the new file to avoid collision, or appends a version indicator. Original file is preserved.				
5	Attempt to delete an attachment on an unlocked experiment. Click the delete icon on the attachment.	Attachment is removed from the entry. A confirmation prompt may appear before deletion. After deletion, the file no longer appears.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	--	------------------------------

OQ-EX-006 Experiment-to-Resource Linking — Bidirectionality

21 CFR Part 11 Reference: 21 CFR 11.10(b): *Records must accurately identify all related materials used.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A Resource record (e.g., a reagent or instrument entry) must exist in the system before this test. Note its ID and title.						
1	Open a test experiment in edit mode. In the body editor, type # followed by the first 3 characters of the resource name.	An autocomplete dropdown appears showing matching resource entries.				
2	Select the resource from the autocomplete list.	The resource is added to the Linked Resources panel on the left/bottom of the experiment. A hyperlink to the resource is inserted in the body text.				
3	Save the experiment. Switch to View mode. Click the link to the resource in the body text.	Browser navigates to the Resource record.				
4	On the Resource record page, navigate to the 'Linked Experiments' or 'Related' section.	The experiment that was linked in Step 2 appears in the Resource's linked entries list. The link is bidirectional.				
5	From the Resource's linked entry panel, click the link back to the experiment.	Browser navigates back to the experiment. Round-trip bidirectional navigation is confirmed.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____	QA Reviewer: _____
-------------------------------	-----------------------	-------------------------------------	------------------------------

OQ-EX-007 Experiment Locking — Prevents Further Modification

21 CFR Part 11 Reference: 21 CFR 11.10(c): After the fact alteration of records must be prevented.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use a test experiment that is ready for locking (all metadata filled, steps completed). Log in as the experiment owner.						
1	Open the test experiment. Click the Lock icon in the toolbar. Confirm the lock action when prompted.	Experiment is locked. A lock icon appears in the experiment header and in the index list view. The lock event is recorded in the Changelog.				
2	Attempt to edit the experiment: click Edit mode and try to modify the title.	Edit mode is not accessible. The experiment is read-only. No modification options are available.				
3	Attempt to add an attachment to the locked experiment.	File upload is rejected. No new attachments can be added to a locked experiment.				
4	Attempt to add a new tag to the locked experiment.	Tag addition is rejected. No new tags can be applied to a locked experiment.				
5	As an Admin (a different user than the owner), navigate to the locked experiment. Attempt to unlock it via the Unlock button in the toolbar.	Admin can unlock the experiment. After unlocking, edit mode becomes accessible again. The unlock event is recorded in the Changelog.				
6	Re-lock the experiment as the Admin.	Experiment is locked again. Lock event recorded in Changelog.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

OQ-EX-008 Experiment Soft Delete and Recovery

21 CFR Part 11 Reference: 21 CFR 11.10(c): Records must be protected from accidental or unauthorized destruction.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Create a dedicated test experiment titled 'OQ-EX-008 Soft Delete Test' for this test.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	Open the test experiment. Navigate to the Ellipsis (...) menu. Click Delete. Confirm the deletion when prompted.	The experiment is removed from the default Experiments index view. It is no longer visible in the normal list.				
2	In the Experiments index, use the State filter to select 'Deleted' or 'Archived' state.	The deleted experiment reappears in the filtered view with 'Deleted' status. The experiment content is fully intact.				
3	Click on the deleted experiment. Verify all content (title, body, metadata, attachments) is intact.	All original content is preserved. The experiment is accessible and readable.				
4	Click Restore (or equivalent) on the deleted experiment.	Experiment is restored to the active index. It is visible again in the default view with its original status.				
5	As SysAdmin, verify that true permanent deletion requires SysAdmin action and cannot be performed by regular users.	Regular User does not see a 'Permanently Delete' option. Only SysAdmin-level actions can perform true permanent deletion (if configured).				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

OQ-EX-009 Full-Text Search Functionality

21 CFR Part 11 Reference: 21 CFR 11.10(e): Records must be available for ready retrieval throughout the retention period.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Create a test experiment with a unique term in both the body text and a metadata field. Use a term unlikely to appear in other records (e.g., 'XQZTEST2026UNIQUE').						
1	Create an experiment. In the body, type: 'XQZTEST2026UNIQUE is documented here.' In a Text metadata field, enter: 'XQZTEST2026META'. Save.	'Experiment is created with the unique terms in both body and metadata.				
2	In the search bar, type: XQZTEST2026UNIQUE and press Enter.	Search results include the test experiment, found by its body text content.				
3	In the search bar, type: XQZTEST2026META and press Enter.	Search results include the test experiment, found by its metadata field content.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Search for a non-existent term: ZZZNORESULT99999.	Search returns zero results. No error message. The empty result state is displayed clearly.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

OQ-EX-010 Experiment PDF Export — Content Completeness

21 CFR Part 11 Reference: 21 CFR 11.10(b): *Records must be complete and accurate.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use a fully populated test experiment (title, date, status, tags, at least 2 metadata fields, body text, 1 completed step, 1 comment, 1 attachment). Note the ELabID of this experiment.						
1	Open the test experiment in view mode. Click the Export button in the toolbar. Select PDF format. Click Export.	'PDF download begins. The file is downloaded to the local machine.				
2	Open the downloaded PDF. Verify the PDF contains the experiment title.	Experiment title is present at the top of the PDF.				
3	Verify the PDF contains the date, status, category, and tags.	All classification fields are present and correct.				
4	Verify the PDF contains all metadata fields and their values.	All metadata field names and values entered in the experiment are present in the PDF.				
5	Verify the PDF contains the body text (main narrative).	Body text content is rendered in the PDF, including any headings, tables, and images that were in the body.				
6	Verify the PDF contains the completed step with its timestamp and tester identity.	Completed step is listed with the correct completion timestamp and tester name.				
7	Verify the ELabID appears in the PDF (typically in the footer).	ELabID is present in the PDF footer or header for cross-referencing.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

4.6 Electronic Signatures [CRITICAL — 21 CFR Part 11 Subpart C: §11.50, §11.70, §11.100, §11.200, §11.300]

21 CFR Part 11 Reference

§11.50: Signed records must include the printed name of the signer, the date and time of signing, and the meaning of the signature. §11.70: Electronic signatures must be linked to their respective records to preclude falsification. §11.100: Electronic signatures must be unique to one individual and not reused or reassigned. §11.200: Electronic signatures shall employ at least two distinct identification components (e.g., ID code and password). §11.300: Controls for identification codes/passwords including use of appropriate controls over their issuance, handling, and periodic revision/recall.

OQ-SIG-001 Simple Electronic Signature — Authenticated Signing Event

21 CFR Part 11 Reference: 21 CFR 11.50(a), 11.70, 11.200(a)(1) — *Non-biometric e-signatures require user ID and password.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use a fully written test experiment in an unlocked state. Log in as the experiment owner (User A).						
1	Open the test experiment in view mode. Click the Signature button in the toolbar. The signature dialog opens.	Signature dialog is displayed. Options are presented for signature type and meaning.				
2	Observe: the dialog requires credential re-entry before signing. Enter User A's password when prompted.	Signing cannot proceed without credential re-entry. The system requires active re-authentication at the point of signing.				
3	Enter the correct password. Select signature meaning (e.g., 'I certify this record is accurate and complete'). Click Sign.	Signature is recorded. A signature block appears in the experiment record showing: (a) the signer's full name, (b) the date and time of signing, (c) the meaning of the signature.				
4	Verify the signature block is appended to the experiment record and visible in view mode.	Signature block is visible with all three required 21 CFR 11.50(a) elements: name, date/time, meaning.				
5	Attempt to remove the signature block by editing the experiment body.	The signature block cannot be deleted from the body by editing. It is rendered as a protected, immutable element.				
6	As a different user (User B), attempt to sign the experiment as if they were User A (use User B's session, enter User B's credentials).	The signature records User B's identity, not User A's. The system does not allow one user to sign as another.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-SIG-002 Electronic Signature — Linking to Record (Cannot Be Detached or Falsified)

21 CFR Part 11 Reference: 21 CFR 11.70: *Electronic signatures must be linked to their respective electronic records so as to preclude the transfer or falsification of the signature.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use the experiment that was signed in OQ-SIG-001.						
1	Open the signed experiment. Observe the signature block. Note the exact text of the signature (name, date/time, meaning).	Signature block is present and displays all required fields.				
2	Unlock the experiment (as Admin). Edit the body text of the experiment. Add additional text after the signature block. Save and re-lock.	Body edit is saved. However, the signature block from OQ-SIG-001 remains and is clearly attributed to the original signing event. The Changelog records the body edit as a new revision, distinct from the signature event.				
3	Navigate to Ellipsis (...) → See Revisions. Compare the pre-edit and post-edit versions.	Revision history shows the original version (as it was when signed) and the post-edit version as distinct entries. The audit trail clearly shows the record was modified after signing.				
4	Export the experiment as a ZIP archive. Inspect the archive contents.	ZIP archive contains: the experiment PDF, a JSON data export, and (if Ed25519 signing was used) the signature archive files. The signature files include the exact content hash at signing time.				
5	Verify that the original signature is still valid against the signing-time snapshot (applicable if Ed25519 cryptographic signing was used; see OQ-SIG-005 for details).	The signature archive preserves the content snapshot at signing time, independent of any subsequent edits to the live record.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-SIG-003 Request Action — Two-Person Review and Countersignature Workflow

21 CFR Part 11 Reference: 21 CFR 11.50(a): Signatures must be associated with specific individuals; 21 CFR 11.70: Signatures linked to records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Two user accounts required: User A (experiment owner/analyst) and User B (reviewer/supervisor). Both must be active members of the same team.						
1	As User A, open a completed, unsigned experiment. Click the Request Action button. Select 'Sign'. In the recipient field, select User B. Add a note: 'Please review and sign as supervisor.' Click Send.	Request Action notification is sent. A confirmation message appears for User A.				
2	As User B, open the notification (Bell icon → notification center). Click the notification for the signature request.	User B is navigated to the experiment awaiting their signature.				
3	As User B, review the experiment content. Click the Signature button in the toolbar. Re-enter User B's password. Select meaning 'Supervisor Review and Approval'. Click Sign.	User B's signature is applied to the experiment. Signature block shows User B's name, date/time, and 'Supervisor Review and Approval' meaning.				
4	Return to User A's session. Navigate to the signed experiment. Observe the signature block.	Both signatures are visible: (1) User A's signature with their details; (2) User B's countersignature with their details. Both are distinct, attributed, and timestamped.				
5	Navigate to the Changelog for this experiment. Verify both signature events are recorded.	Changelog entries show two signature events: one attributed to User A, one to User B. Each has a unique timestamp and cannot be altered.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-SIG-004 Electronic Signature — Uniqueness and Non-Repudiation

21 CFR Part 11 Reference: 21 CFR 11.100(a): Each electronic signature shall be unique to one individual and shall not be reused by or reassigned to another individual.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Two user accounts (User A and User B) are required. This test verifies that electronic signatures can only be applied using the account holder's credentials.						
1	Log in as User A. Open an unsigned experiment. Click Signature. In the credential re-entry dialog, enter User B's password instead of User A's.	Authentication fails. The signature is not applied. An error message indicates invalid credentials.				
2	Enter User A's correct password. Sign with meaning 'Author Certification'.	Signature is applied. The signature block shows User A's name.				
3	Log out as User A. Log in as User B. Navigate to the experiment signed by User A. Observe the signature.	The signature block shows User A's name, not User B's. User B cannot delete, modify, or claim ownership of User A's signature.				
4	As User B, attempt to add a second signature to the same experiment claiming to be User A (enter User A's credentials in User B's browser session).	The system rejects the attempt: the credentials are checked against the current authenticated session. The signature would be attributed to User B, not User A.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-SIG-005 Ed25519 Cryptographic Signature — Signing and Archive Creation

21 CFR Part 11 Reference: 21 CFR 11.70: Electronic signatures must be linked to records to preclude falsification. Ed25519 provides cryptographic non-repudiation.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: This test applies only if Ed25519 cryptographic signing is enabled. User must have generated an Ed25519 key pair in Settings → Account → Cryptographic Key. Skip this test and mark N/A if only simple signatures are used.						
1	In Settings → Account, verify the Ed25519 public key is generated and displayed. Note the key fingerprint.	Public key fingerprint is displayed. No errors.				
2	Open a test experiment. Click Signature → Ed25519 (cryptographic signature) option. Enter the passphrase protecting the private key. Select meaning	Signature process executes. A 'Signature created' confirmation appears. An immutable ZIP archive (the signature archive) is attached to the experiment in				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	'Cryptographic Author Certification'. Click Sign.	an archived/hidden attachment state.				
3	Navigate to Ellipsis (...) → Show Archived Attachments (or equivalent). Locate the signature archive ZIP.	The signature archive is present. Its filename includes the signature date/time and user identifier.				
4	Download the signature archive ZIP. Extract it. Verify it contains: (a) data.json (the experiment snapshot at signing time); (b) a .minisig signature file; (c) a public key file; (d) a verify.sh or README verification script.	All four components are present in the archive.				
5	Execute the verification script or manually verify using Minisign: minisign -Vm data.json -p publickey.pub -x signature.minisig	Verification output: 'Signature and comment signature verified.' The data.json content matches the experiment state at the time of signing.				
6	Modify data.json (add one character). Re-run verification.	Verification fails: 'Signature verification failed.' This demonstrates that any alteration of the signed content is detectable.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

4.7 Trusted Timestamping [CRITICAL — 21 CFR 11.10(c), 11.70]

21 CFR Part 11 Reference

21 CFR 11.10(c): Protection of records to enable accurate and ready retrieval; 21 CFR 11.70: Signatures/stamps linked to records. RFC 3161 timestamps provide independent, third-party-certified proof of prior existence, protecting against backdating of records.

OQ-TS-001 RFC 3161 Timestamp — Application and Token Storage

21 CFR Part 11 Reference: 21 CFR 11.10(c): Records must be retrievable in accurate form; timestamps establish temporal integrity.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: The TSA endpoint must be configured in Sysconfig → Timestamping. Internet access to the TSA is required. A test experiment in an unlocked state is required.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	Open the test experiment in view mode. Click the Timestamp button (clock/seal icon) in the toolbar. Observe the process.	A timestamp request is initiated. A progress indicator or confirmation message appears. No error messages.				
2	After the timestamp completes, navigate to Ellipsis (...) → Show Archived Attachments.	A timestamp archive file (.zip or similar) appears in the archived attachments list. Its creation timestamp is the current date and time.				
3	Download the timestamp archive. Inspect its contents.	Archive contains: (a) the experiment JSON snapshot at timestamp time; (b) a .tsr (timestamp response) token file from the TSA; (c) a README or metadata file identifying the TSA used.				
4	Verify the TSA token is from the configured TSA provider (e.g., DFN.de, DigiCert, Sectigo). Inspect the .tsr file using: openssl ts -reply -in timestamp.tsr -text	TSA name, policy, hash algorithm (SHA-256), and timestamp are displayed. The timestamp matches the date/time of the timestamp application.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

OQ-TS-002 Timestamp Hash Integrity — Pre- and Post-Timestamp Content Verification

21 CFR Part 11 Reference: 21 CFR 11.10(c): Records must be protected from alteration or falsification.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use the timestamped experiment from OQ-TS-001. This test verifies that: (1) the content hash in the token matches the actual content at timestamp time; (2) subsequent modifications are detectable.						
1	From the timestamp archive (OQ-TS-001, Step 3), extract the experiment JSON file (data.json or equivalent). Compute its SHA-256 hash: sha256sum data.json	Record the computed SHA-256 hash: [_____] _____]				
2	Extract the .tsr token file. Verify the hash embedded in the token: openssl ts -reply -in timestamp.tsr -text grep 'Message imprint'	The hash shown in the TSA token exactly matches the SHA-256 hash computed in Step 1. This confirms the token was issued for this specific content.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
3	Unlock the experiment. Add additional text to the body. Save and re-lock. Re-export the experiment to JSON or ZIP.	New export/JSON is created. Its content is different from the pre-modification snapshot.				
4	Compute the SHA-256 hash of the new export. Compare to the hash in the original timestamp token.	The new hash is DIFFERENT from the hash in the original timestamp token. This demonstrates that the timestamp token is specific to the pre-modification content. The modification is detectable.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

4.8 Audit Trail [CRITICAL — 21 CFR 11.10(e)]

21 CFR Part 11 Reference

21 CFR 11.10(e): Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

OQ-AT-001 Changelog — Field Change Attribution and Timestamp

21 CFR Part 11 Reference: *21 CFR 11.10(e): Audit trails must record date/time, user identity, and what was changed.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Log in as User A. Create or open a test experiment. Record its current title before making changes.						
1	Open a test experiment in edit mode. Note the current title. Change the title to a new value (e.g., add ' — MODIFIED' at the end). Save.	Title is changed successfully.				
2	Navigate to Ellipsis (...) → See Changelog.	Changelog page opens and displays a list of change events.				
3	Locate the most recent entry. Verify it shows: (a) the field that changed ('title'); (b) the previous value (original title); (c) the new value (modified	All five data elements are present and accurate for the title change.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	title); (d) the identity of the user who made the change (User A); (e) the date and time of the change.					
4	Change the experiment's Status. Save. Return to the Changelog.	A new changelog entry appears for the status change, also including all five data elements.				
5	Attempt to delete or modify a Changelog entry. Look for any edit, delete, or modify option on the Changelog.	No option exists to edit or delete any Changelog entry. The Changelog is read-only and immutable.				
6	Add a metadata field value. Change a tag. Return to the Changelog.	Both the metadata field change and the tag change appear as distinct entries in the Changelog.				

Performed By:	Date:	Result (Pass/Fail):	QA Reviewer:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

OQ-AT-002 Revisions — Main Text Body Version History

21 CFR Part 11 Reference: 21 CFR 11.10(e): Audit trail must capture all modifications to electronic records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Create a new test experiment with initial body text. Then make at least two subsequent edits to create a multi-version history.						
1	Create an experiment with body text: 'Version 1 content — original text.' Save.	Experiment is saved.				
2	Edit the body text: change 'Version 1 content' to 'Version 2 content — first edit.' Save.	Change is saved.				
3	Edit the body text again: add a new paragraph 'Version 3 addition.' Save.	Change is saved.				
4	Navigate to Ellipsis (...) → See Revisions.	Revisions page opens. A list of at least 3 revisions (initial + 2 edits) is displayed, each with a timestamp and the user identity of the editor.				
5	Click on Version 1 (the earliest revision).	The body text content for Version 1 is displayed exactly as it was when first				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
		saved: 'Version 1 content — original text.'				
6	View the diff between Version 1 and Version 2 (if diff view is available).	Added and removed text is highlighted. Changes are clearly visible between versions.				
7	Attempt to delete any revision entry.	No option exists to delete revision history. Revisions are immutable.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-AT-003 ELabID — Uniqueness and Immutability

21 CFR Part 11 Reference: 21 CFR 11.10(b): Record accuracy and uniqueness; permanent record identification.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Three test experiments are needed for this test.						
1	Create three separate experiments. Navigate to the bottom of each experiment in view mode. Record the ELabID for each.	ELabID 1: _____] ELabID 2: _____] ELabID 3: _____ _____				
2	Compare the three ELabIDs.	All three ELabIDs are unique. No two experiments share the same ELabID.				
3	Attempt to modify the ELabID of one experiment by editing any available field.	No field in the user interface allows modification of the ELabID. It is a system-generated, read-only identifier.				
4	Delete one of the experiments (soft delete). Create a new experiment. Verify the new experiment's ELabID.	The new experiment has a new unique ELabID. The ELabID of the deleted experiment is not reused or reassigned.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-AT-004 System Audit Log — Authentication and Admin Events**21 CFR Part 11 Reference:** 21 CFR 11.10(e): Audit trail must capture all access and administrative actions.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: SysAdmin access required. Perform a deliberate set of auditable actions before checking the log.						
1	Perform these actions in sequence: (a) Log in as a test user; (b) Log out; (c) Attempt login with wrong password; (d) As SysAdmin, modify a configuration setting in Sysconfig.	All actions are performed.				
2	As SysAdmin, navigate to Sysconfig → Logs.	The system audit log page is accessible. Filtering options are available.				
3	Filter the log for the test user's login events from the past hour.	Successful login event and logout event for the test user are both present, each with timestamp and IP address.				
4	Filter for failed login attempts.	The failed login attempt (wrong password) appears with timestamp and IP address.				
5	Filter for SysAdmin configuration change events.	The configuration change made in Step 1(d) appears in the log with the SysAdmin's identity and timestamp.				
6	Attempt to delete any log entry.	No option exists to delete any log entry. The system audit log is immutable.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

OQ-AT-005 Audit Trail Completeness — Multi-Step Workflow Record**21 CFR Part 11 Reference:** 21 CFR 11.10(e): Audit trail must record a complete and accurate account of all actions.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: This test verifies that a complete chain of events across a full experiment lifecycle is captured without gaps. Perform the following workflow sequentially on a new test experiment.						
1	As User A, create a new experiment titled 'OQ-AT-005 Completeness Test'. Save.	Record creation is logged in Changelog.				
2	Add a tag 'AT-Test'. Save.	Tag addition is logged.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
3	Change status to 'Running' (if not default). Save.	Status change logged.				
4	Add a comment: 'OQ completeness test comment.' Save.	Comment creation logged.				
5	Upload an attachment.	Upload event logged.				
6	Apply an electronic signature (any type).	Signature event logged.				
7	Apply an RFC 3161 timestamp.	Timestamp event logged.				
8	Lock the experiment.	Lock event logged.				
9	Navigate to Ellipsis → See Changelog. Count the entries.	Changelog contains at least 8 entries corresponding to the 8 actions above. Each entry has: event type, previous value (where applicable), new value, user identity, and timestamp. No actions are missing from the record.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

4.9 Template Management [HIGH]

OQ-TM-001 Team Template Creation and Team-Wide Availability

21 CFR Part 11 Reference: 21 CFR 11.10(b): Standardized procedures for generating accurate and complete records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Log in as Admin for this test. A regular User account (non-Admin) must be available for Step 5.						
1	As Admin, navigate to Experiments → Templates. Click Create. Enter template name: 'OQ-TM-001 Validation Template'. Select category. Add body text: 'Section: Results'. Add two metadata fields: (1) 'Analyst Name' (Text); (2) 'Result' (Select: Pass, Fail). Add one locked step: 'Step 1: Review all data before signing.' Mark the step	Template is created and saved without error.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	as locked. Click Make available to Team. Save.					
2	As Admin, navigate to Experiments → Templates. Search for 'OQ-TM-001 Validation Template'.	Template appears in the templates list with the team-visible indicator.				
3	As Admin, create a new experiment. When the template selection dialog opens, search for 'OQ-TM-001 Validation Template'.	The template appears in the template selection dialog.				
4	As a regular User (non-Admin), log in. Navigate to Experiments → Create. Open the template selection dialog.	The template 'OQ-TM-001 Validation Template' is visible to the regular User in the template selection list.				
5	As the regular User, create an experiment from the template.	New experiment opens with: (a) 'Section: Results' in the body; (b) 'Analyst Name' and 'Result' metadata fields; (c) 'Step 1' in the steps panel with a lock icon indicating it is locked.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

OQ-TM-002 Template Locked Steps Cannot Be Modified by User

21 CFR Part 11 Reference: 21 CFR 11.10(b): Standardized procedures; 11.10(e): Controls ensure procedural compliance.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Use an experiment created from OQ-TM-001 template (which has one locked step). Log in as the experiment owner (regular User, not Admin).						
1	Open the experiment in edit mode. Locate the locked step 'Step 1: Review all data before signing.'	Locked step is visible. A lock icon is displayed on or near the step. The step text is not editable.				
2	Attempt to click on the locked step text and type replacement text.	The text field is non-editable. No modification is accepted.				
3	Attempt to delete the locked step by clicking any delete icon or using keyboard delete.	No delete option is available for the locked step. The step cannot be removed.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Attempt to drag-and-drop the locked step to a different position in the steps list.	Step position cannot be changed. Locked step remains in its original position.				
5	Click the checkbox on the locked step to mark it as complete.	Step completion is accepted. The step is marked as complete with a timestamp and user attribution. Only the checkbox (completion) is interactive, not the step text.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
------------------------	----------------	--	--------------------------------

4.10 Resource Management [MEDIUM-HIGH]

OQ-RM-001 Resource Creation and Category Assignment

21 CFR Part 11 Reference: 21 CFR 11.10(b): Accurate cataloging of all materials used in GxP records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: At least one Resource Category must exist in the system. Log in as a regular User.						
1	Navigate to Resources. Click Create. Enter title: 'OQ-RM-001 Test Reagent Lot'. Select a resource category.	Resource creation dialog accepts title and category.				
2	Add a metadata text field with key 'Lot Number' and value 'LOT-OQ-2026-001'. Add a date field 'Expiry Date' with today's date + 365 days. Save.	Resource is created and all fields are saved correctly.				
3	Navigate to the Resources index. Filter by the category used in Step 1.	The newly created resource appears in the filtered index.				
4	Search for 'OQ-RM-001' in the search bar.	The resource appears in search results, findable by title.				
5	Open the resource in view mode. Verify all fields (title, category, metadata fields) are displayed correctly.	All fields display the correct values entered in Steps 1 and 2.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-RM-002 Resource Scheduler — Booking and Conflict Prevention

21 CFR Part 11 Reference: 21 CFR 11.10(b): Records accurately reflect when controlled items are used.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A bookable resource (e.g., an instrument with scheduling enabled) must exist. Admin must have enabled booking on the resource. Log in as a regular User.						
1	Navigate to Resources. Open a bookable resource. Click 'Book Item' or navigate to the Scheduler.	The scheduler/calendar view opens showing the resource's availability.				
2	Click on an available time slot for tomorrow (e.g., 10:00 AM – 12:00 PM). Add a booking note: 'OQ-RM-002 Test Booking'. Confirm.	Booking is created. The time slot appears in the calendar as occupied with the booking user's name.				
3	As a second user (User B), attempt to book the same resource for the same time slot.	Booking conflict is detected. User B receives an error or warning indicating the time slot is already booked. The booking is not created.				
4	As User A, cancel the test booking.	Booking is cancelled. The time slot becomes available again.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

4.11 User and Team Administration [HIGH]

OQ-UA-001 User Account Validation Workflow

21 CFR Part 11 Reference: 21 CFR 11.10(d): Access limited to authorized individuals only.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Self-registration must be enabled in the Team settings (Admin Panel → Team tab) for this test. Require Admin validation of new accounts must also be enabled.						
1	From a browser not logged in, navigate to the ELabELN registration page. Register a	Registration is accepted. A message indicates the account is pending Admin				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	new test account with a valid email address.	validation and cannot be used until validated.				
2	Attempt to log in with the newly registered account before Admin validation.	Login fails. Error message indicates the account is pending validation. Access is denied.				
3	As Admin, open the Admin Panel → Users tab. Locate the pending new account.	Pending account appears in a 'Validation pending' list or state.				
4	As Admin, click Validate for the new account.	Account is activated. The status changes to active/validated.				
5	Attempt login with the newly validated account credentials.	Login succeeds. User is redirected to the ELabELN dashboard.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-UA-002 Team Export — Bulk Experiment Data Integrity

21 CFR Part 11 Reference: 21 CFR 11.10(c): Records must be accurately and readily retrievable throughout the retention period.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Admin account required. At least 5 experiments of a specific category must exist.						
1	As Admin, navigate to Admin Panel → Export. Select experiment export. Filter by category = [test category]. Select PDF format. Click Export.	Export process begins. Progress may be indicated.				
2	After the export completes, download the output (ZIP or individual PDFs).	Files download successfully. Number of files matches the number of experiments in the selected category.				
3	Open one of the exported PDFs. Verify it contains the experiment's title, date, metadata, and body content.	PDF content is complete and matches the experiment's actual content in ELabELN.				
4	Verify the ELabID appears in the PDF footer.	ELabID is present, enabling cross-reference between the paper PDF and the digital record.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

4.12 System Configuration and Integration [MEDIUM]

OQ-SC-001 REST API — Authentication and Read Operation

21 CFR Part 11 Reference: 21 CFR 11.70: *Electronic records must be accessible through authenticated methods only.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Generate a read-only API key in Settings → API Keys before this test. Record the key value.						
1	Execute: curl -H 'Authorization: [API_KEY]' https://[SERVER_NAME]/api/v2/users/me	Returns HTTP 200 with a JSON object containing the authenticated user's name, email, and team. Authentication via API key is successful.				
2	Execute: curl -H 'Authorization: INVALID_KEY_VALUE' https://[SERVER_NAME]/api/v2/users/me	Returns HTTP 401 Unauthorized. Invalid API keys are rejected.				
3	Execute: curl -H 'Authorization: [API_KEY]' https://[SERVER_NAME]/api/v2/experiments?limit=5	Returns HTTP 200 with a JSON array of up to 5 experiments accessible to the API key's user.				
4	Using a Read-Only API key, attempt to create a new experiment: curl -X POST -H 'Authorization: [READ_ONLY_KEY]' https://[SERVER_NAME]/api/v2/experiments	Returns HTTP 403 Forbidden. Read-only keys cannot create or modify records.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____ _____
-------------------------------	-----------------------	---	---------------------------------------

OQ-SC-002 Timestamping Service Configuration Verification

21 CFR Part 11 Reference: 21 CFR 11.10(c): *Protection of records; trusted third-party temporal integrity.*

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: SysAdmin account required. Verify the TSA is configured in Sysconfig → Timestamping.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	As SysAdmin, navigate to Sysconfig → Timestamping. Verify the configured TSA URL matches the approved TSA from Section 2.4.	TSA URL matches the configured value in Section 2.4.				
2	Create a test experiment. Apply an RFC 3161 timestamp (see OQ-TS-001).	Timestamp is applied without error, confirming the TSA endpoint is reachable and the configuration is valid.				
3	From the timestamp archive, confirm the TSA certificate chain can be verified. Execute: openssl ts -reply -in [timestamp.tsr] -text grep 'TSA'	TSA identity is displayed and matches the configured provider.				

Performed By: _____	Date: _____	Result (Pass/Fail): _____ _____ _____	QA Reviewer: _____
-------------------------------	-----------------------	---	------------------------------

4.13 OQ Summary

OQ Summary Item	Recorded Value
Total OQ Test Cases	[Record: _____]
CRITICAL Tests — Passed	[Record: _____] / [Total CRITICAL: _____]
HIGH Tests — Passed	[Record: _____] / [Total HIGH: _____]
MEDIUM Tests — Passed	[Record: _____] / [Total MEDIUM: _____]
Total Tests Failed	[Record: _____] — Deviation IDs: [_____]
N/A Tests	[Record: _____] — (List N/A IDs: _____)
Open Deviations	[Record: _____] — All deviations documented in Appendix D
OQ Overall Result	PASS / FAIL / CONDITIONAL PASS (circle one)

Role	Name	OQ Approval Signature / Date
Validation Owner	[Name / Title]	[Signature / Date]
QA Reviewer	[Name / Title]	[Signature / Date]

Section 5: Performance Qualification (PQ)

The Performance Qualification demonstrates that ELabELN operates correctly and consistently under actual use conditions with real users performing real workflows. PQ scenarios are designed to replicate complete end-to-end laboratory workflows that span multiple system features and confirm the system performs appropriately as an integrated whole.

PQ Prerequisites: (1) IQ and OQ are complete and approved. (2) The system is configured with production-representative data (at least one team, categories, templates, and user accounts). (3) All PQ testers are trained ELabELN users who have completed any required onboarding. (4) PQ is conducted in the production environment (or an exact copy of it for initial validation).

PQ-001: Complete Regulated Analytical Experiment Lifecycle

Objective: Demonstrate that a complete GxP-compliant analytical experiment record can be created, documented, reviewed, signed, timestamped, and locked in a workflow that satisfies all 21 CFR Part 11 requirements simultaneously.

Compliance Significance

This scenario tests the entire 21 CFR Part 11 compliance chain in a single workflow: authentication (11.10(d)), complete record generation (11.10(b)), contemporaneous documentation (11.10(e)), electronic signature (11.50), signature linkage to record (11.70), trusted timestamp (11.10(c)), and final locking (11.10(c)).

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Two users required: Analyst (User A) and Supervisor (User B). A method validation or analytical run template must exist with at least 4 metadata fields and 3 steps (at least 1 locked).						
1	As the Analyst, log in with personal credentials (MFA if required). Create a new experiment from the analytical template. Title: 'PQ-001 HPLC Potency — Sample Batch PQ-2026'. Set date to today.	Experiment created from template. All template fields present.				
2	Fill all metadata fields: Analyst = [tester name], Instrument = [instrument ID], Lot Number = [test lot], Result = [a representative numeric value], Pass/Fail = Pass.	All metadata fields populated and saved.				
3	Write a protocol summary in the body text (at least 3 sentences describing the analytical procedure performed).	Body text saved and visible in view mode.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
4	Upload a test file ('PQ-001-rawdata.pdf') as an attachment.	File attached successfully. Upload timestamp and analyst identity shown.				
5	Complete all protocol steps by clicking each checkbox. Verify each step shows a completion timestamp and the Analyst's name.	All steps completed and timestamped. Each step shows Analyst identity.				
6	Apply an electronic signature with meaning 'I certify this record is accurate, complete, and was prepared by me personally.' Re-enter credentials when prompted.	Signature block appears with Analyst name, date/time, and meaning.				
7	Use Request Action → Sign to request the Supervisor's countersignature. As the Supervisor, review the experiment and apply a countersignature with meaning 'Supervisor Review and Technical Approval.'	Supervisor signature block added. Both signatures are visible and individually attributed.				
8	Apply an RFC 3161 timestamp. Verify the timestamp archive is created (Ellipsis → Archived Attachments).	Timestamp archive is present with today's date.				
9	Lock the experiment.	Experiment is locked. Lock event appears in Changelog.				
10	Navigate to the Changelog. Verify all 10 events from this workflow are present in the audit trail (creation, field edits, file upload, step completions, two signatures, timestamp, lock).	Changelog contains at least 10 entries covering all workflow events. Each entry has timestamp and user identity. No gaps in the chain of events.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-002: Multi-User Concurrent Access and Data Isolation

Objective: Demonstrate that multiple users can simultaneously use the system without data collision, that private records remain isolated, and that all concurrent actions are individually attributed.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Three simultaneous user sessions required (three computers or browsers). Users: Analyst A, Analyst B, Admin C. All in the same team.						
1	Simultaneously: Analyst A creates an experiment titled 'PQ-002-UserA-Concurrent'. Analyst B creates 'PQ-002-UserB-Concurrent'. Admin C opens the team experiment index.	All three operations succeed simultaneously without error or interference.				
2	Analyst A sets their experiment to 'Only Me' privacy. Analyst B sets theirs to 'My Team'. Both save.	Both privacy settings are accepted.				
3	Analyst B's session: navigate to the index. Search for 'PQ-002-UserA-Concurrent'.	Analyst B CANNOT see Analyst A's private experiment in search results.				
4	Admin C's session: navigate to the index (with Admin view of all team experiments). Search for 'PQ-002-UserA-Concurrent'.	Admin C CAN see Analyst A's private experiment (Admin privilege). The experiment is present in Admin C's view.				
5	Simultaneously: Analyst A adds a tag, Analyst B changes a status, Admin C exports a different experiment. All three perform their actions at the same time.	All three operations succeed without error. Each change is applied to the correct experiment.				
6	Verify the Changelog for each experiment shows the correct user identity for each change.	Each experiment's Changelog shows only the attributed user's changes. No cross-attribution errors.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-003: Template Enforcement Consistency Across Users

Objective: Demonstrate that a team template with locked steps produces identical structure and enforcement for all users who create experiments from it, regardless of which user creates the experiment.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Three different user accounts (all regular Users, not Admin). OQ-TM-001 template must exist with at least one locked step.						
1	User A creates an experiment from the OQ-TM-001 template. Record the step descriptions as User A sees them.	Experiment created. Steps listed: [Record step 1 text: _____]				
2	User B creates a separate experiment from the same template. Compare the steps to User A's.	Steps are identical: same text, same order, same lock status as User A's.				
3	User C creates a third experiment from the same template.	Steps are identical to Users A and B.				
4	All three users attempt to modify the locked step description on their respective experiments.	All three fail. Locked step is non-editable for all three users.				
5	All three users complete their locked steps by clicking the checkbox. Verify each completion shows that user's individual identity and a unique timestamp.	Each completion is individually attributed: User A's step shows User A, User B's shows User B, User C's shows User C. All timestamps are distinct.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-004: Audit Trail Integrity Under Sequential Edits by Multiple Users

Objective: Demonstrate that the audit trail captures a complete, unbroken chain of events when multiple users make sequential modifications to the same experiment record.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: One shared experiment (write access for multiple users). Three users: User A (owner), User B (editor), User C (editor). Note the experiment ELabID.						
1	User A creates experiment 'PQ-004-MultiUser-AuditTest' with initial body text 'Initial content by User A.' Set	Experiment created. Changelog shows creation by User A.				

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
	permission to allow User B and C to edit. Save.					
2	User B edits the title to append ' — Updated by B'. Saves.	Title update saved. Changelog entry: User B changed title.				
3	User C adds a metadata field value. Saves.	Metadata update saved. Changelog entry: User C changed metadata.				
4	User A changes the body text (adding a new paragraph). Saves.	Body text revision created. Revisions shows new version by User A.				
5	User B adds a comment: 'PQ-004 comment by User B.'	Comment added. Comment panel shows User B's name and timestamp.				
6	User A locks the experiment.	Lock event recorded in Changelog with User A's identity.				
7	Navigate to the Changelog for this experiment.	Changelog shows 5+ distinct entries in chronological order: creation (A), title change (B), metadata change (C), lock (A). Each entry has the correct user attribution and timestamp. No events are missing.				
8	Navigate to Revisions. Verify the body text revision history.	Revision history shows the initial version (User A) and the modified version (User A, Step 4). User B and C's changes (non-body) are in Changelog but not Revisions (correct behavior).				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-005: Resource Traceability — Lot Impact Analysis

Objective: Demonstrate that a single resource record can be linked to multiple experiments and that the complete list of linked experiments is retrievable from the resource record for impact analysis purposes.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A Resource record (e.g., a reagent lot) and 10 test experiments must be available. Batch linking via the API or manual linking of 10 experiments is acceptable.						
1	Open the Resource record 'OQ-RM-001 Test Reagent Lot' (created in OQ-RM-001). Record its ID.	Resource record is open. ID:				
2	Link 10 different experiments to this resource (either via the body text # autocomplete or the Links panel). Verify each link is created.	All 10 experiments are linked to the resource. Each linking operation succeeds.				
3	Open the resource record in view mode. Navigate to the Linked Experiments or Related section.	A list of linked experiments appears. All 10 experiments that were linked in Step 2 are visible in this list.				
4	Click on one linked experiment from the resource. Navigate to the experiment.	Navigation to the experiment is successful. The experiment's Links panel shows the resource.				
5	From the experiment, click the link back to the resource.	Navigation back to the resource is successful. Round-trip bidirectional navigation confirmed.				
6	Search for 'OQ-RM-001 Test Reagent Lot' in the main search bar.	Search results include the resource record as a top result.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable):

PQ-006: Backup and Restore Integrity

Objective: Demonstrate that the backup and restore procedure produces complete, accurate, and retrievable records — satisfying 21 CFR Part 11 requirement 11.10(c) for record protection and accessibility.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: This test requires system administrator access. Schedule this during a maintenance window as it involves container restarts. For sciCloud.net® deployments, coordinate with LabLynx support.						

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
1	Create a test experiment titled 'PQ-006-BackupRestoreTest' with: body text, 2 metadata fields, 1 attachment, 1 completed step, 1 comment, 1 signature. Note the ELabID.	Test experiment created. ELabID: _____				
2	Execute the backup procedure: sudo /usr/local/bin/elab-backup.sh (or elabctl backup run). Verify completion with no errors.	Backup completes successfully. Backup directory contains DB dump and uploads backup.				
3	Soft-delete the test experiment from ELabELN. Verify it disappears from the active index.	Experiment is no longer visible in the default experiment index.				
4	Stop the ELabELN containers: cd /etc/elabftw && sudo docker compose down	Containers stop cleanly.				
5	Restore the database from backup: zcat [backup]/elabftw-db.sql.gz sudo docker exec -i mysql mysql -u elabftw -p[password] elabftw. Restore uploads: sudo rsync -av --delete [backup]/uploads/ /var/elabftw/web/	Restore commands execute without errors.				
6	Restart ELabELN: sudo docker compose up -d. Wait for healthy status.	Both containers start and report healthy.				
7	Log in. Navigate to the experiments index. Search for 'PQ-006-BackupRestoreTest'. Verify all content is restored.	Experiment is present in the index. All content (body text, metadata, attachment, step completion, comment, signature) is intact and matches the pre-backup state.				
8	Navigate to the Changelog of the restored experiment. Verify the signature event is present.	All audit trail events are intact post-restore. The signature event is preserved with its original timestamp and attribution.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]

Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []
------------------------	--

PQ-007: System Recovery After Unplanned Restart

Objective: Demonstrate that ELabELN recovers cleanly from an unplanned server restart, that containers auto-restart, and that no data is lost or corrupted.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: Requires system administrator access. For sciCloud.net®, coordinate with LabLynx support. Note the current state of several experiments before the test.						
1	Record the titles and last-saved timestamps of 3 existing experiments.	Record: Exp 1: [] Exp 2: [] Exp 3: []				
2	Simulate an unplanned restart: sudo reboot (or LabLynx-managed equivalent for sciCloud.net®). Wait for the server to complete the reboot cycle (typically 2–5 minutes).	Server reboots and comes back online.				
3	After reboot, wait 3 minutes. Execute: sudo docker ps	Both elabftw and mysql containers show 'Up' status with healthy health check. Containers auto-started without manual intervention.				
4	Navigate to ELabELN in a browser. Log in with valid credentials.	Login page loads. Login succeeds. Dashboard is accessible.				
5	Navigate to the three experiments recorded in Step 1. Verify their titles, last-saved timestamps, and content are unchanged.	All three experiments are present with their original content. No data has been lost or corrupted.				
6	Navigate to the Changelog of one of the three experiments. Verify the audit trail is intact.	Changelog shows all pre-restart events. No audit trail entries are missing.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-008: API Integration — Programmatic Record Creation and Audit Trail

Objective: Demonstrate that experiments created programmatically via the REST API are indistinguishable from UI-created records in the audit trail, and that all 21 CFR Part 11 controls apply equally to API-created records.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: A valid Read-Write API key must be available. Python with the requests library, or curl, must be available on the testing workstation.						
1	Execute via API: POST /api/v2/experiments. Note the returned experiment ID from the Location header.	API returns HTTP 201 Created. Record experiment ID: [_____]				
2	Execute via API: PATCH /api/v2/experiments/{id} with body: {"title": "PQ-008 API Integration Test", "date": "[today]", "metadata": {"extra_fields":{"Analyst":{"type":"text","value":"API-Integration-Test"}}}}.	API returns HTTP 200. Metadata field is populated.				
3	Execute via API: POST /api/v2/experiments/{id}/tags with body {"tag": "PQ-API-Test"}	API returns HTTP 201. Tag is added.				
4	In the ELabELN browser interface, navigate to the experiment created in Step 1. Verify it appears in the index with the correct title and tag.	Experiment is visible in the UI with all API-set values.				
5	Navigate to the Changelog of the API-created experiment.	Changelog shows creation event attributed to the user associated with the API key, with a system timestamp. Tag addition event also recorded.				
6	In the UI, apply an electronic signature to the API-created experiment (with credential re-entry). Verify signature is applied.	Signature is applied and recorded exactly as for a UI-created experiment. The system treats API-created and UI-created records identically.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[_____]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): [_____]

PQ-009: Data Archival and Long-Term Retrievability

Objective: Demonstrate that archived experiments remain fully accessible, searchable, and retrievable, and that archived records maintain complete audit trail integrity.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: At least 10 completed, signed experiments must be available for archiving. This test simulates project closure archival.						
1	As Admin, navigate to Admin Panel → Batch Actions. Select 'Archive' action. Filter to select 10 completed experiments from a specific category. Preview the action.	Preview shows the correct 10 experiments. No unintended experiments are included.				
2	Execute the batch archive action.	10 experiments are archived. They no longer appear in the default experiment index.				
3	In the Experiments index, use the State filter to select 'Archived'.	All 10 archived experiments appear in the filtered view.				
4	Open one archived experiment. Verify all content (body, metadata, attachments, steps, comments, signatures, Changelog) is intact.	All content is preserved exactly as it was before archiving.				
5	Search for one archived experiment by title (without the archived filter).	Archived experiments may or may not appear in default search (depends on configuration). With the archived state filter enabled, the experiment is findable.				
6	Attempt to edit an archived experiment.	Edit is not permitted on archived experiments. The record is protected from modification.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

PQ-010: Deviation and Incident Scenario — Post-Signature Modification Detection

Objective: Demonstrate that the system's controls correctly detect and document any attempt to modify a signed and locked record, and that the audit trail provides an accurate and complete record of the modification chain.

Step	Action / Procedure	Expected Result	Actual Result	P/F	Initials	Date
Prerequisites / Notes: This scenario simulates a real-world deviation scenario: a record that was signed and locked is subsequently unlocked and modified (a scenario that would require a formal change control in a GMP environment). The test verifies the audit trail captures all events accurately.						
1	Create a new experiment. Populate all fields. Sign (Analyst). Apply RFC 3161 timestamp. Lock. Record the experiment title and ELabID.	Experiment signed, timestamped, and locked. ELabID: []				
2	As Admin, unlock the experiment. (Record the reason in the Deviation Log, Appendix D). Note the unlock timestamp.	Experiment is unlocked. Unlock event appears in Changelog with Admin identity and timestamp.				
3	Add a corrective note to the body text: 'Correction per Deviation DEV-OQ-PQ10: [describe correction]'. Save.	Body text modified. New revision created in Revisions history.				
4	Re-apply the Analyst signature and the Supervisor signature (new signing events for the corrected record).	Two new signature events appear. The original signatures and the new signatures are all visible in the record.				
5	Re-apply an RFC 3161 timestamp (to the corrected record).	New timestamp archive created. The original timestamp archive is also preserved (archived attachment from Step 1).				
6	Re-lock the experiment.	Experiment locked. Re-lock event in Changelog.				
7	Navigate to the Changelog. Verify it shows the complete chain: creation, original signing, original timestamp, lock, UNLOCK, body edit, new signatures, new timestamp, re-lock — in chronological order with all events attributed.	The Changelog shows a complete, unbroken chain of all 10+ events. The unlock event is clearly visible, the modification is attributed to the Admin, and all post-correction signatures are separately attributed. No events are hidden or missing. The record accurately reflects everything that happened.				

Field	Value
PQ Scenario Performed By	[Name / Title / Signature]
Date of Execution	[]
QA Observer / Reviewer	[Name / Title / Signature]
Scenario Result	PASS / FAIL (circle one) — Deviation Ref (if applicable): []

5.2 PQ Summary

PQ Summary Item	Recorded Value
Total PQ Scenarios	10
Scenarios Passed	[Record: _____]
Scenarios Failed	[Record: _____] — Deviation IDs: [_____]
Open Deviations	[Record: _____] — All deviations documented in Appendix D
PQ Overall Result	PASS / FAIL / CONDITIONAL PASS (circle one)

Role	Name	PQ Approval Signature / Date
Validation Owner	[Name / Title]	[Signature / Date]
QA Reviewer	[Name / Title]	[Signature / Date]

Section 6: Change Control and Revalidation Requirements

21 CFR Part 11 and GAMP 5 require that validated computerized systems be maintained in a validated state throughout their operational lifetime. Any change to the system must be assessed for its impact on validation status, and appropriate revalidation must be performed before the change is placed in production use.

6.1 Change Control Trigger Criteria

Change Type	Revalidation Requirement
ELabELN Version Upgrade (minor: x.x.X)	Review release notes. Assess impact on validated functions. Execute regression OQ for any changed or potentially impacted features. Full revalidation not typically required for minor patch updates, but a documented risk assessment is mandatory.
ELabELN Version Upgrade (major/minor: X.x.0 or x.X.0)	Full OQ repeat for all CRITICAL and HIGH-risk functions. PQ-001 through PQ-005 minimum. Update System Baseline (Section 2). Update IQ for any changed infrastructure.
Configuration Change (new category, template, status)	Document the change. Execute the relevant OQ test cases for the changed configuration element (e.g., OQ-TM-001/002 for a new template). Minimal revalidation may be sufficient.
Authentication Change (new SSO provider, MFA enforcement)	Execute OQ-AC-001 through OQ-AC-004 for the new authentication path.
Infrastructure Change (new server, OS upgrade, Docker upgrade)	Full IQ repeat. Execute OQ-AT-004/005 (audit log continuity). Execute PQ-007 (restart recovery).
Network or TLS Certificate Change	Execute IQ-005 and IQ-006. Verify application accessibility and API connectivity.
Backup System Change	Execute IQ-010 and PQ-006.
sciCloud.net® Platform Update (LabLynx-managed)	LabLynx is responsible for infrastructure change control. Customer must receive notification of changes and LabLynx's qualification documentation. Customer executes application-level OQ/PQ regression as warranted.

Section 7: Validation Summary Report

Complete this section after all IQ, OQ, and PQ testing is complete and all deviations have been resolved or risk-accepted by QA. This section constitutes the formal conclusion of the validation exercise.

7.1 Summary of Validation Results

Summary Element	Recorded Value
System Name and Version	ELabELN — Version: [_____]
Validation Period	From: [___ / ___ / ___] To: [___ / ___ / ___]
IQ Result	PASS / FAIL / CONDITIONAL PASS — Tests: [____] Passed / [____] Failed / [____] N/A
OQ Result	PASS / FAIL / CONDITIONAL PASS — Tests: [____] Passed / [____] Failed / [____] N/A
PQ Result	PASS / FAIL / CONDITIONAL PASS — Scenarios: [____] Passed / [____] Failed
Total Open Deviations	[____] Critical / [____] Major / [____] Minor — All closed: Yes / No
Overall Validation Result	VALIDATED / NOT VALIDATED / CONDITIONALLY VALIDATED (circle one)
Conditional Use Restrictions (if applicable)	[Describe any restrictions on system use pending CAPA completion: _____]

7.2 21 CFR Part 11 Compliance Attestation

Based on the test evidence documented in this validation package, the following attestation is made regarding ELabELN's compliance with 21 CFR Part 11:

21 CFR Part 11 Section	Compliance Evidence References
§11.10(a) — Validation	ELabELN has been validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. Evidence: IQ-001 through IQ-014; OQ-EX-007, OQ-EX-008; PQ-001 through PQ-010.
§11.10(b) — Record Legibility and Retention	Electronic records are accurate and complete. They can be accurately and readily retrieved throughout the records retention period. Evidence: OQ-EX-010, OQ-SC-001, PQ-005, PQ-009.
§11.10(c) — Record Protection	Computer-generated audit trails prevent loss or modification of records. Backup procedures protect records for retrieval during the retention period. Evidence: OQ-EX-007, OQ-AT-001 through OQ-AT-005, PQ-006.
§11.10(d) — Access Limitation	System access is limited to authorized individuals. Evidence: OQ-AC-001 through OQ-AC-007; IQ-005, IQ-012, IQ-013.

§11.10(e) — Audit Trails	Secure, computer-generated, time-stamped audit trails independently record operator entries and actions. Evidence: OQ-AT-001 through OQ-AT-005, PQ-004, PQ-010.
§11.30 — Open Networks	Records transmitted via open networks (HTTPS) include measures to ensure authenticity, integrity, and confidentiality. Evidence: IQ-005, IQ-006; OQ-SC-001.
§11.50 — Signature Manifestations	Signed electronic records contain the printed name, date/time, and meaning of the signature. Evidence: OQ-SIG-001, OQ-SIG-003.
§11.70 — Signature Linkage	Electronic signatures are linked to their electronic records to preclude transfer or falsification. Evidence: OQ-SIG-002, OQ-SIG-005, PQ-010.
§11.100 — Signature Uniqueness	Each electronic signature is unique to one individual and not reused or reassigned. Evidence: OQ-SIG-004.
§11.200 — Signature Components	Non-biometric signatures employ at least two distinct identification components (user ID + password / + MFA). Evidence: OQ-AC-001, OQ-AC-003, OQ-SIG-001.
§11.300 — Signature Controls	Controls ensure only genuine owners use their signatures; systems detect attempted misuse. Evidence: OQ-AC-002, OQ-SIG-004.

7.3 Final Approval and Release

By signing below, the approvers confirm that: (1) all validation testing has been completed as documented in this package; (2) all deviations have been resolved or risk-accepted; (3) ELabELN is released for use in the generation and maintenance of electronic records subject to 21 CFR Part 11; and (4) this validation package is retained as a controlled record for the life of the system.

Role	Name / Title	Final Approval Signature / Date
Validation Owner	[Name / Title]	[Signature / Date]
Quality Assurance Director	[Name / Title]	[Signature / Date]
System Owner / IT Director	[Name / Title]	[Signature / Date]
Department Head / VP R&D	[Name / Title]	[Signature / Date]
Regulatory Affairs (if applicable)	[Name / Title]	[Signature / Date]

Appendix A: 21 CFR Part 11 Traceability Matrix

21 CFR §	Requirement Summary	Test Cases Providing Evidence
§11.10(a)	Validation	IQ-001-014; OQ-EX-001-010; OQ-SIG-001-005; OQ-TS-001-002; OQ-AT-001-005; PQ-001-010
§11.10(b)	Accurate/Complete Records	OQ-EX-001,002,003,005,010; OQ-TM-001,002; OQ-RM-001; PQ-001,003,005
§11.10(c)	Record Protection	OQ-EX-007,008; OQ-AT-001-005; OQ-TS-001,002; IQ-010; PQ-006,009
§11.10(d)	Access Controls	OQ-AC-001-007; IQ-005,012,013; PQ-002
§11.10(e)	Audit Trails	OQ-AT-001-005; OQ-EX-004; PQ-004,010
§11.30	Open Networks / Encryption	IQ-005,006; OQ-SC-001
§11.50	Signature Manifestations	OQ-SIG-001,003; PQ-001
§11.70	Signature Linkage to Record	OQ-SIG-002,005; OQ-TS-002; PQ-010
§11.100	Signature Uniqueness	OQ-SIG-004; PQ-003
§11.200	Signature Components	OQ-AC-001,003; OQ-SIG-001
§11.300	Signature Controls	OQ-AC-002; OQ-SIG-004

Appendix B: Deviation Log Template

Use one form per deviation. Assign sequential deviation numbers: DEV-[DocumentNumber]-[SequentialNumber] (e.g., DEV-VLD-ELAB-001-01).

Field	Value
Deviation Number	DEV-_____
Date of Deviation	[__ / __ / __]
Validation Phase	IQ / OQ / PQ (circle one)
Test Case ID	[e.g., OQ-SIG-001]
Step Number	[Step ____]
Description of Deviation	[Describe exactly what occurred vs. what was expected: _____]
Expected Result (from protocol)	[Exact text from Expected Result column: _____]
Actual Result Observed	[Exact text of what was observed: _____]
Deviation Classification	Critical / Major / Minor (circle one)
Immediate Impact Assessment	[Does this deviation prevent system use for GxP records? Yes / No. Justification: ____]
Root Cause Investigation	[Describe root cause: _____]
CAPA Required	Yes / No (circle one)
CAPA Description (if required)	[Describe corrective and preventive action taken: _____]
Retest Required	Yes / No (circle one)
Retest Result	PASS / FAIL / N/A (circle one)
Resolution Date	[__ / __ / __]
QA Approval	[QA Reviewer Name / Signature / Date]

Appendix C: Abbreviations and Definitions

Abbreviation / Term	Definition
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available — data integrity framework.
CAPA	Corrective and Preventive Action. Documented response to a deviation, identifying root cause and actions to prevent recurrence.
CFR	Code of Federal Regulations (United States).
CSV	Computer System Validation. The formal process for demonstrating that a computerized system consistently produces a result meeting predetermined specifications.
ELN	Electronic Laboratory Notebook.
GAMP 5	Good Automated Manufacturing Practice guidance for validation of automated systems, published by ISPE. Version 5 (2nd Edition) is the current reference.
GLP	Good Laboratory Practice.
GMP	Good Manufacturing Practice.
GxP	Collective term for Good [x] Practices (GLP, GMP, GCP, etc.).
IQ	Installation Qualification — documented verification that equipment/software has been installed correctly.
MFA	Multi-Factor Authentication — authentication requiring two or more verification factors.
OQ	Operational Qualification — documented verification that equipment/software operates according to its specifications.
PQ	Performance Qualification — documented verification that equipment/software consistently performs according to specifications under actual conditions of use.
RFC 3161	Internet Standard for trusted timestamping, providing independent third-party verification of document existence at a specific time.
SOC 2	Service Organization Control 2 — audit standard for service providers covering security, availability, processing integrity, confidentiality, and privacy.
TSA	Timestamp Authority — a trusted third party that issues RFC 3161 timestamp tokens.
URS	User Requirements Specification — document defining the functional and non-functional requirements that a system must meet.
21 CFR Part 11	Title 21 of the U.S. Code of Federal Regulations, Part 11 — Electronic Records; Electronic Signatures. FDA regulation.

Appendix D: Referenced Documents

Document	Author	Reference / Location
21 CFR Part 11 (1997)	FDA	Electronic Records; Electronic Signatures. 62 FR 13430. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11
FDA Guidance — Part 11, ERR, ES (2003)	FDA	Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application. https://www.fda.gov/regulatory-information/search-fda-guidance-documents
FDA Guidance — Computerized Systems in Clinical Investigations (1999)	FDA	Guidance for Industry: Computerized Systems Used in Clinical Investigations.
GAMP 5 (2nd Edition, 2022)	ISPE	Good Automated Manufacturing Practice (GAMP) 5: A Risk-Based Approach to Compliant GxP Computerized Systems.
ICH Q9(R1) Quality Risk Management	ICH	Harmonised Tripartite Guideline — Quality Risk Management.
ELabELN User Manual v3.0	LabLynx	Complete feature reference for users. Produced by LabLynx, Inc.
ELabELN Administrator Manual v1.0	LabLynx	Team and system administration reference. Produced by LabLynx, Inc.
ELabELN Developer Manual v1.0	LabLynx	REST API reference and integration guide. Produced by LabLynx, Inc.
ELabELN License, TechSpecs & Installation Manual v1.0	LabLynx	Software stack, installation, and technical specifications. Produced by LabLynx, Inc.
RFC 3161 — Time-Stamp Protocol (TSP)	IETF	Internet X.509 Public Key Infrastructure Time-Stamp Protocol. https://www.rfc-editor.org/rfc/rfc3161



ELabELN — IQ/OQ/PQ Validation Manual | VLD-ELAB-001

21 CFR Part 11 / GAMP 5 Category 4

LabLynx, Inc. | www.lablynx.com | support@lablynx.com | www.elabeln.com
© 2026 LabLynx, Inc. | **CONFIDENTIAL — CONTROLLED DOCUMENT** | All rights reserved.